

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK**

---

NETWORK DATA ROOMS, LLC,

X

Civil Case No.: 22-CV-2299-LGS

Plaintiff,

-v-

SAULREALISM LLC and RYAN SAUL, in her individual and professional capacities,

Defendants.

X

---

**DECLARATION OF DAVID DELORGE IN SUPPORT OF PLAINTIFF NETWORK DATA ROOMS, LLC'S MOTION FOR A PRELIMINARY INJUNCTION**

DAVID DELORGE, pursuant to 28 U.S.C § 1746, hereby declares as follows:

1. Since approximately, November 2020, I have worked as a consultant for plaintiff Network Data Rooms, LLC ("NDR") in the role of DealTable Azure Chief Cloud Architect and Cloud Security Engineer in connection with NDR's longtime development project for the creation of a highly secure, innovative and technologically advanced virtual data room platform ("DealTable VDR Platform").
2. I have worked in the information technology (IT) industry for almost 30 years, have a Masters in Technology, hold multiple cloud certifications, am a Microsoft Certified Professional and a Security cloud architect and have extensive knowledge and experience in Microsoft Azure DevOps.
3. Prior to working for NDR, I signed a nondisclosure agreement and a consulting agreement that acknowledged the confidentiality of, *inter alia*, NDR's information, trade secrets, software and code, related to the DealTable VDR Platform project and acknowledging that NDR is the owner of all services and code created as part of the project.

4. In my role as DealTable Azure Chief Cloud Architect and Cloud Security Engineer, I am responsible for overseeing the infrastructure platform on which DealTable VDR Platform is being built, making sure that all services and code were being backed up and had high availability and governance, and in implementing and monitoring security protocols.

5. Defendant Ryan Saul (“Saul”), who NDR retained as a consultant in December 2020, to work as lead project developer, reported to me and NDR’s members involved in the project. Saul was primarily responsible for editing the existing codebase of the software underlying the DealTable VDR Platform and writing new source code for the features and functionality of the DealTable VDR Platform. I worked with Saul on the servers, databases and web services that operated based on the source code created by Saul, and assisted with the manual testing and maintenance of the DealTable VDR Platform being built.

6. Until August 2021, there were multiple code developers working on the project and all work and tasks related to the source code were being tracked on the Azure DevOps Repository Boards and Task program.

7. As part of the development project, I was responsible for establishing NDR’s Azure DevOps Source Code Repository, which is NDR’s secure, restricted access repository for its source code, where all developers working on the DealTable VDR Platform software development project are required to “check in” a/k/a save all source code.

8. In addition, I made sure that NDR’s DealTable VDR Platform used every available security precaution to protect its codebase and source code being created as part of the development project including full backups, secure accessibility, Privileged Identity Management, Data Loss Prevention and Virtual Desktops.

9. These security measures include the following:

(i) The ‘DealTable.com’ website was configured with NIST, SSL, TTLS 1.2, secure connections, monitoring using Microsoft Azure Application Insights, Log Analytics and Azure Sentinel. Full access report from location, GEO and latency, Backup and Recovery applied and full auditing using Microsoft Defender and Compliance Manager. All Microsoft services were backed up and had disaster recovery features enabled.

(ii) The ‘DealTable’ application was configured with the following security and compliance settings: NIST, PII, SPI, GDPR, UDPR, SOC. All data was encrypted, disaster recovery and replication enforced, GEO redundant and Role Base Access, PIM enabled, along with MFA, Multi factor authentication, Trusted locations, Identity Risk and full Azure Sentinel NOC dashboard.

(iii) ‘DealTable’ Infrastructure Security consisted of Azure Information Protection, Azure Advanced Security, Azure Log analytics, Logic Apps, Conditional Access, Network Security, Azure Application Gateway, DR, Backup, Alerting, NOC Dashboard and compliance reviews and certifications, Microsoft auditing reviews and full privileged access reviews and roles.

(iv) Privileged Identity Management.

(v) Assignment of Azure Virtual Desktops to each developer to ensure the security of the DealTable Software and its development project.

10. Pursuant to NDR’s established security protocols, Saul was required to always use the Azure Active Directory User account in order to access the DealTable VDR Platform codebase and source code and as a second level of security to prevent unauthorized access to the data and applications an Azure Multi-Factor Authentication process was deployed.

11. In addition, Saul was provided with a secure internet connection through the Azure Virtual Desktop assigned to her and from which she was required to perform all work on the codebase and source code for DealTable VDR Platform.

12. Defendant Saul was provided access to the codebase for the DealTable VDR Platform solely for the purpose of carrying out her duties as Lead Developer and directed Saul to check in all code work she performed into NDR's secure Azure DevOps Source Code Repository.

13. Beginning in September 2021, Saul became the only developer working on the project and she requested to work through Microsoft Teams for maintaining a shared list of tasks with me and the NDR's members, Chris Concannon and Thomas Concannon.

14. Despite the alteration in how coding changes were being tracked, Saul was at all times required to perform all coding work on her assigned Azure Virtual Desktop and save all source code on NDR's secure Azure DevOps Source Code Repository.

15. By way of background, original source code for a website or webapplication, its features and functionality, are written by a coder on a development site and saved on a secured repository. This source code is originally in a decompiled format and can be edited, built upon, and updated. When this source code is compiled and deployed to a production site, it becomes the performance-based code read by a computer that is encompassed and viewable on a website or webapplication. Specifically, the features of a website or webapplication consist of compiled code and cannot be edited or updated. All updates or additions to the features must be made to the decompiled format of the code a/k/a original source code.

16. Following the events that gave rise to this action, it was discovered that the original source code written by defendant Saul between September 26, 2021 and January 18, 2022 was never saved by Saul on NDR's secure Azure DevOps Source Code Repository.

17. Following my review of the DealTable systems, I have determined that Saul, without authorization, downloaded NDR's codebase for the DealTable VDR Platform to a self-owned GitHub Repository and, beginning on September 26, 2021 performed her coding work

including changes to the source code and the creation of new code to build out the DealTable VDR Platform on a personal computer and saved the source code on a hidden, self-owned GitHub Repository, which violated the security procedures implemented by NDR.

18. Neither I, nor NDR's members were aware of Saul's actions, nor did we consent to them. In fact, Saul went to great lengths to conceal her unlawful conduct in downloading the codebase for the DealTable VDR Platform and not working from her assigned Azure Virtual Desktop by logging in to the Virtual Desktop each day but actually coding on a different machine. In addition, Saul created a new "branch" on NDR's secure Azure DevOps Source Code Repository called "Ryan Development," where she told me that source code was being saved and, instead, uploaded old code to the repository so that I and NDR's members would believe that she was uploading the new source code that was being deployed to the DealTable VDR platform website and application. *See* email from Ryan Saul dated October 20, 2021 annexed hereto as Exhibit "A."

19. The decompiled source code created by Saul between September 26, 2021 and January 18, 2022 and missing from NDR's secure Azure DevOps Source Code Repository represents critical features and functionality of the DealTable VDR Platform, consisting of the following:

- Office documentation editing
- PDF redaction
- Roles, Permissions, and Group Editing
- Single Sign On
- Time out of application
- Database connectivity
- Upload documentation function, singularly and/or bulk upload
- Workflows
- Ability to edit the Deal Setting
- Project settings
- Analytics and Reporting
- Multifactor authentication for login
- Application advanced settings, Color, Images , Fonts
- Archiving of documents
- Document tree and Library
- Activity log

20. Instead, NDR’s secure Azure DevOps Source Code Repository only has the decompiled source code written prior to September 26, 2021, which does not include the original source code for the aforementioned features. If pre-September 26, 2021 decompiled source code is “deployed” to the production site, it will override the existing production site and all the features and functionality presently available on the DealTable website and webapplication will be lost.

21. Saul’s unlawful retention of the decompiled source code prevents NDR from adding additional features, editing existing features or from making any future updates. Consequently, Saul’s actions have paralyzed NDR’s ability to complete the project and launch the DealTable VDR Platform, which it has been working towards for the last three years, and on January 18, 2022, was only a month or two from completing.

#### **Events of January 18, 2022**

22. In preparation for a check-in meeting scheduled for the morning of January 18, Thomas Concannon sent Saul an extensive list of open and new code edits that needed to be made to the DealTable VDR Platform codebase in order to complete the software development project.

23. On the morning of January 18, 2022, I received a text message from Saul stating that she “had” to talk with me “ASAP.”

24. I spoke with Saul and she was angry about the list of tasks that Thomas sent to her. During the call, Saul threatened to delete the DealTable VDR Platform [Dev Code] in order to upset NDR’s members, Chris Concannon and Thomas Concannon and to force them to do what she wanted.

25. I immediately told Saul that she could not delete the codebase and that doing so is a felony and a breach of the Consulting Agreement and NDA she signed with NDR.

26. I did not believe that she would really delete the codebase so, at the time, I did not tell Chris and Thomas Concannon about Saul's threats. I now wish I had.

27. Later in the day, Saul and Chris Concannon had a disagreement regarding Saul's performance and negative and volatile attitude and Chris terminated Saul from the project. Chris Concannon then directed me to immediately block Saul's access to NDR's Microsoft Azure DevOps and NDR's Azure DevOps Source Code Repository, which I immediately did.

28. A few hours later, I, Chris and Thomas Concannon, and Saul had a virtual meeting, during which Saul apologized for her behavior and asked to be permitted to continue working on the project as the Lead Developer.

29. Chris Concannon agreed to allowing her to continue on the project and directed me to reinstate her access to NDR's Microsoft Azure DevOps and NDR's Azure DevOps Source Code Repository.

30. During a conference call held later that same day between me, Chris and Thomas Concannon and Saul, Saul became belligerent and Chris Concannon, again, fired her from the project.

31. After Saul hung up, Chris Concannon directed me to again block her access to NDR's Microsoft Azure DevOps and NDR's Azure DevOps Source Code Repository.

32. The process for blocking someone's access to NDR's Microsoft Azure DevOps and NDR's Azure DevOps Source Code Repository takes less than one minute to complete but during this time, Saul launched a small bat file that deleted the DealTable website and marketing site, the DealTable application, the DealTable database and database connection, the DealTable website certificates, and the current permissions and user data, and she attempted to create a back door into the Network Security.

33. After discovering what Saul had done, I was able to restore the deleted databases and websites by retrieving the Disaster Recovery back-ups and manually restoring the connections and re-installing the certifications, Microsoft Office apps and PDF apps. However, I was only able to partially restore the DealTable application, but was not able to restore the database connection.

34. In reviewing the Disaster Recovery back-ups, I discovered that Saul had embedded re-write code in the database at 9:50 a.m. on January 18, 2022 and had removed all administrative privileges to the Webapp in order to prevent me and NDR from accessing the Webapp.

35. At approximately 4:00 p.m. MST, Saul called me and admitted to having deleted the DealTable services because according to Saul “they deserved it.” I told Saul what she did was wrong and not to contact me again. Saul then asked me for a reference, which I did not respond to. Before hanging up, Saul asked me to tell the Chris and Thomas Concannon that she “could fix it” if they wanted her to continue as lead developer for the project.

36. I took all the necessary steps to block, remove and add Saul’s IP and location to NDR’s security blocks and while monitoring the security of the system, I could see that Saul made several attempts to unlawfully regain access to NDR’s DealTable systems.

37. NDR informed me that it was filing a criminal complaint against Saul for cybercrimes with the New York District Attorney’s Office and the Federal Bureau of Investigations related to the deletion of the DealTable database and Webapplications, and I was asked to provide a summary of Saul’s unlawful conduct. It is my understanding that the investigation is ongoing.

38. In the weeks following Saul’s termination from the project and in reviewing the code currently stored in NDR’s Azure DevOps Source Code Repository, on or around February 17, 2022, I discovered that the last time Saul checked in source code to NDR’s Azure DevOps

Source Code Repository was on September 26, 2021 and none of the code written by Saul between September 26, 2022 and January 18, 2022 had been saved on NDR's repository.

39. After discovering that Saul downloaded NDR's original codebase for the DealTable VDR Platform to her personal repository and has stolen the source code created between September 26, 2021 and January 18, 2022, NDR notified the authorities of Saul's additional crimes.

40. In addition, I have called, emailed, and texted Saul on numerous occasions to ask that she return the source code but she has refused to respond to any of my attempts to contact her and remains in wrongful possession of NDR's source code.

41. The source code in NDR's repository represents 80% of the codebase needed to finish the development of the DealTable VDR Platform. The missing source code from September 26, 2021 through January 18, 2022 is necessary in order for NDR to make the edits and updates needed to the source code to complete the development of the DealTable VDR Platform.

42. The stolen decompiled source code constitutes a trade secret of NDR because it is the basis for the additional features that make the DealTable VDR platform superior to its competitors and will provide NDR with a competitive advantage over existing virtual data room providers.

43. None of the virtual data rooms on the market contain all the features that will be offered by the DealTable software. For instance, there are currently three virtual data room providers on the market that would be considered NDR competitors. These competitors' virtual data rooms lack the following functions: (i) Chat embedded functionality, (ii) redaction restrictions, (iii) increased security through multi-factor authenticated logins, (iv) ability to edit

and save documents directly on the platform, (v) ability to draft and drop documents for uploads, or a (vi) adequate user interface and intuitive user experience.

44. NDR's DealTable VDR Platform would be offered at a lower price point than one competitor and, while it may be at a higher or comparable price point to the other two competitors, it would be a superior product, with technologically advanced features, and easier to use.

45. The more time that Saul is allowed to maintain possession and control of NDR's source code, the greater the possibility that she may destroy it or disclose it to NDR's competitors.

46. This would be extremely harmful to NDR because without its code, it would likely take NDR's competitors years to replicate and install the features of the DealTable VDR platform into their existing virtual data room platforms.

47. In fact, prior to commencing this litigation, NDR retained the services of a Full Stack developer to try to rebuild the missing decompiled source code but he was unable to do so and NDR had to terminate his services. If NDR does not recover the decompiled source code, it would be virtually impossible to have a new developer replicate it because each coder has a unique way of coding and the existing codebase saved on the development site was written by Saul, who did not comment or on her code, or use Classes in writing the code, making it very difficult for a new code developer to understand its functionality in order to write new code that can be pieced together with the saved codebase.

48. Accordingly, NDR's motion for a temporary restraining order and preliminary injunction should be granted.

49. I declare under the penalty of perjury that the foregoing is true and correct.

Dated: March 22, 2022

DAVID DELORGE